WHITEHAT3 PROJECT

킥오프 보고서

AWS 환경에서의 보안 모범사례 가이드 및 점검 자동화

IAM Root

목차 LIST

01 팀 소개

멘토

이주호

PL

안가은

PM

정보경

팀원

박병우

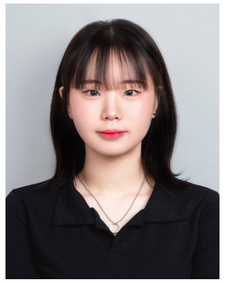
박나현

나경민

이승찬

김정우

김채영



이수현

02 프로젝트 개요

프로젝트 정의

AWS 기반 인프라를 실제 운영 환경에 가깝게 구성하고,
보안 및 컴플라이언스 상태를 자동으로 점검하며,
그 결과를 실시간으로 시각화하고 알림까지 연동할 수 있는 클라우드
보안 자동화 시스템을 구축합니다.

02 프로젝트 개요

프로젝트 목표

초기에는 AWS의 서비스로 인프라를 구성하고, 보안 그룹 설정, IAM 정책 등을 통해 기본 보안 설정을 체계화합니다.

이후에는 정책 자동화 도구를 활용하여 설정 위반 사항을 점검, 리소스 자동 종료 및 알림 기능 등 자동 대응 로직을 도입하고, 시각화 도구를 통해 점검 결과와 이벤트를 모니터링하고, 협업 툴과 연동하여 알림 체계를 구성합니다.

이와 함께 악의적, 실수성 시나리오를 설계하여 실제로 대응 흐름을 검증하고, 최종적으로는 보안 리포트를 자동으로 생성하고 공유할 수 있는 기능까지 구현합니다.

02 프로젝트 개요

프로젝트 목표

이를 통해 운영자가 직접 개입하지 않아도 보안 상태를 지속적으로 점검하고,
위협 요소에 대해 선제적으로 대응할 수 있는 자동화 기반의 보안 운영 환경을
구현함으로써 시나리오 기반 보안 사고 대응까지 자동화하는 통합 보안 시스템을
구축합니다.

03 프로젝트 용어 정의

IAM (Identity and Access Management)	AWS에서 사용자, 그룹, 권한을 관리하는 서비스로, 안전한 리소스 접근 제어의 핵심 도구
Security Hub	AWS 내 다양한 보안 서비스 결과를 통합해 보안 상태를 시각화하고, 권고사항을 제공하는 대시보드형 서비스
AWS Config	리소스의 구성 변경을 추적하고, 규정 위반 여부를 자동으로 평가해주는 서비스
Lambda	서버 없이 코드를 실행할 수 있는 컴퓨팅 서비스로, 이벤트 기반 자동화에 주로 활용
VPC (Virtual Private Cloud)	AWS 상에 사용자가 정의한 가상 네트워크로, 리소스 간 통신과 보안 설정의 기본 단위가 됨

04 프로젝트 필요성

2024 .env파일 → AWS 자격증명 유출

2024 노출된 .env 파일을 통해 AWS 자격증명이 유출되었고, 공격자는 이를 기반으로 권한 상승, 악성 Lambda 배포, S3 데이터 탈취까지 자동화된 방식으로 공격을 수행했으며, 전체 과정에서 탐지나 차단이 이루어지지 않아 피해가 확산되었습니다.

2024 Shiny Hunters 해킹 사례

2024년 Shiny Hunters 해킹 사례는 수작업 점검으로는 자격증명 노출이나 권한 설정 오류 같은 인적 실수를 신속히 발견하기 어렵다는 한계를 보여줬습니다. 개발자들이 실수로 공개 저장소에 AWS 접근 키를 업로드한 것을 수동체계에서 놓치면서, 대규모 데이터 유출이 발생했습니다.

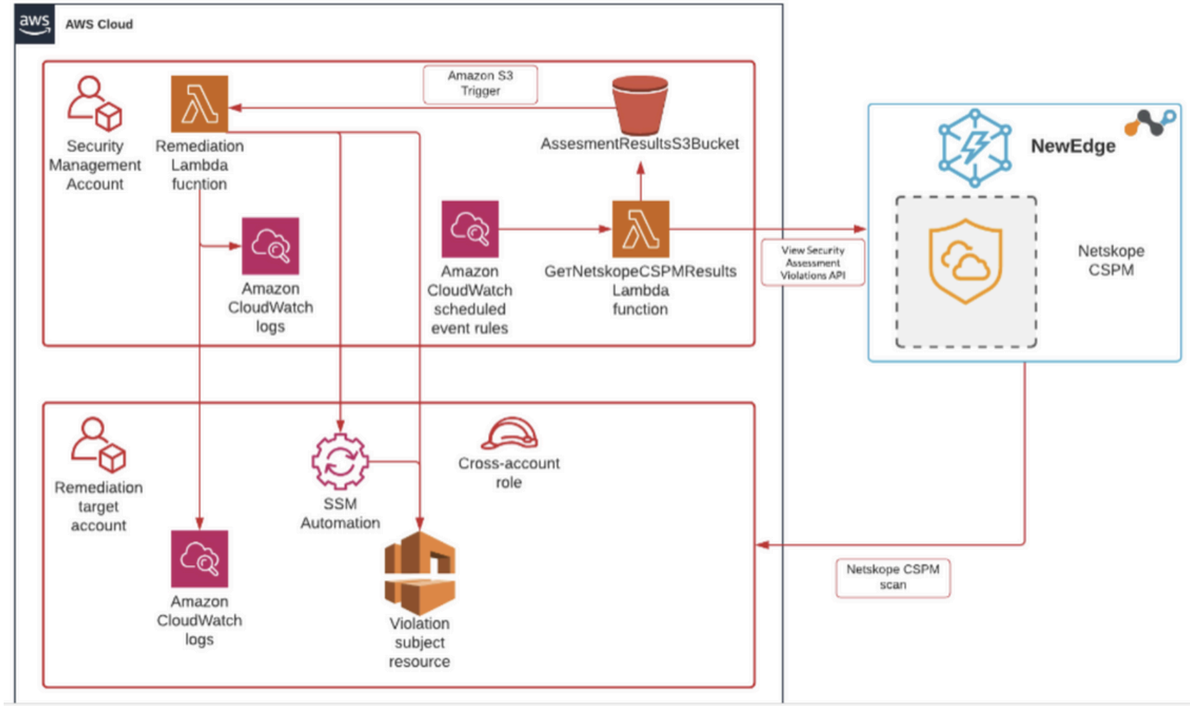
2024 글로벌 기업 AWS 자격증명 유출

Datadog와 Mandiant 같은 주요 글로벌 기업들도 AWS 자격증명 유출로 인한 보안 사고를 경험했습니다. Datadog는 피싱 공격을, Mandiant는 예전 직원의 클라우드 자격증명의 유출로 인한 피해를 입었습니다.

추진 배경

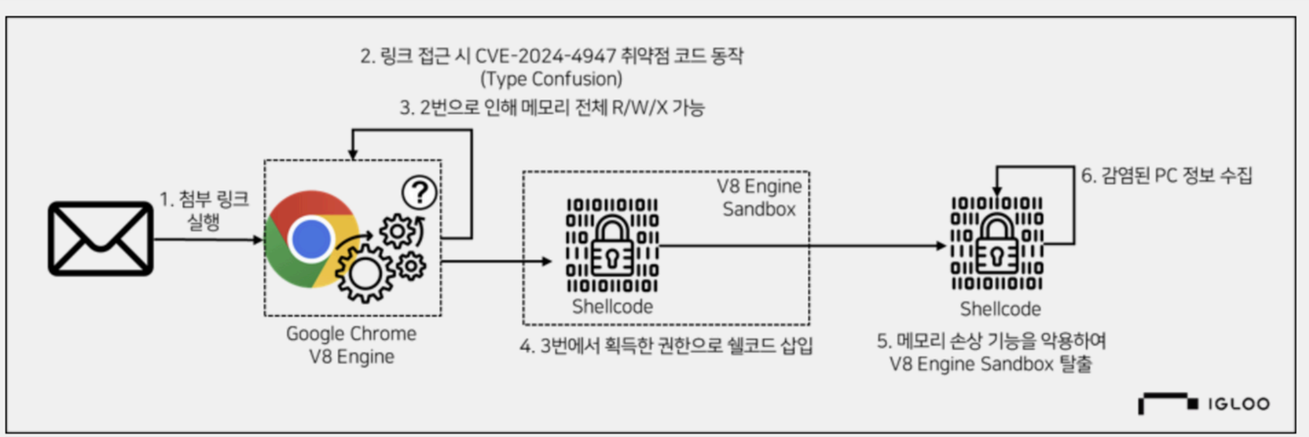
보안 위협 증가에 따른 실시간 대응 미흡
수작업 점검의 위험성
실무형 역량 부족

05 프로젝트 차별성



기존의 보안 자동화 프로젝트들은 대체로 AWS Security Hub, Config, Lambda를 활용하여 사전에 정의된 정책에 따라 리소스를 점검하고, 그 결과를 단순 리포트 형태로 제공하는 데 그치는 경우가 많음.

05 프로젝트 차별성



[그림 4] Kaspersky Blog 내용을 기반으로 재구성한 공격 구성도

단순한 점검 수준을 넘어, 시나리오 기반의 보안 사고 대응까지 자동화하는 통합 보안 시스템 구축을 목표로 하고 있음.

이를 위해 최근 3년 이내 발생한 인프라 해킹 사례 및 악성코드 공격 트렌드를 조사하고,
주요 보안 기업들이 개발 중인 클라우드 보안 기술을 분석하여 실효성 있는 자동 대응 구조를 설계하고자 함.

05 프로젝트 차별성

또한, Slack, Discord 등의 협업 툴과의 연동을 통해 완전 자동화 흐름을 구현할 예정

“보안 사고 감지 → 실시간 알림 → 시각화 → 정기 보고서 자동 생성”

slack + 

06 프로젝트 수행계획

내용	2025.05				2025.06				2025.07				2025.08			
	1주	2주	3주	4주	1주	2주	3주	4주	1주	2주	3주	4주	1주	2주	3주	4주
프로젝트 준비 및 환경 세팅																
인프라 및 기본 보안 구성																
자동 점검 및 대응 로직 구현																
시나리오 기반 보안 대응 설계																
모니터링 및 시각화 환경 구축																
통합 테스트 및 발표 준비																

06 프로젝트 수행계획

프로젝트 준비 및 환경 세팅 (5월 1일 ~ 5월 8일))

팀 역할 분담 및 커뮤니케이션 채널 구성

프로젝트 목표 및 범위 구체화

AWS 계정 생성, IAM 권한 정리, 환경 구축 준비

인프라 및 기본 보안 구성 (5월 9일 ~ 5월 22일)

EC2, S3, VPC, Load Balancer 등 주요 리소스 구성

보안 그룹 및 IAM 정책 설정

AWS Config, CloudTrail, Security Hub 기본 설정

06 프로젝트 수행계획

자동 점검 및 대응 로직 구현 (5월 23일 ~ 6월 7일)

정책 기반 리소스 점검 자동화 (Lambda 활용)

위반 시 자동 조치 로직 개발 (종료, 격리, 태그 변경 등)

정기 리포트 자동 생성 기능 설계

시나리오 기반 보안 대응 설계 (6월 8일 ~ 6월 21일)

최근 인프라 사고 분석

탐지 → 대응 → 알림 흐름 자동화 구현
보안 기업 기술 벤치마킹

Slack/Discord 연동 알림 기능 개발

06 프로젝트 수행계획

모니터링 및 시각화 환경 구축 (6월 22일 ~ 7월 10일)

CloudWatch, EventBridge, Grafana 등 시각화 연동

실시간 자원 상태 대시보드 구성

이벤트 기반 로그/경고 시각화 자동화

통합 테스트 및 발표 준비 (7월 11일 ~ 8월 1일)

전체 시나리오 기반 종합 테스트

보고서 자동화 및 최종 문서 정리

발표자료 제작 및 데모 시연 준비

07 결론

실질적인 보안 대응력 확보

단순 점검을 넘어, 시나리오 기반 감지 및 대응까지 자동화한 통합 시스템 구축

실무 수준의 보안 사고 재현 및 자동 처리 경험 확보

다양한 AWS 서비스의 실전 활용

EC2, S3, CloudWatch, Lambda, IAM, Config 등

AWS 자원에 대한 직접 구성, 연동, 트러블슈팅 능력 강화

시각화 · 협업 연동으로 가시성 향상

Slack/Discord 연동으로 실시간 알림, 상황 공유

대시보드 구성 및 보고서 자동화로 운영 편의성까지 확보

감사합니다.